

Procedures for Deregistration Officials and Account Sponsors

May 2000



National Institutes of Health
Center for Information Technology
NIH Computer Center
12 South Drive MSC 5607
Bethesda, Maryland 20892-5607

Publication No. CIT150A

TABLE OF CONTENTS

EXECUTIVE SUMMARY	3
Note for Non-NIH Users:	3
ORIENTATION.....	4
About the Center for Information Technology (CIT).....	4
About the Office of the Deputy Chief Information Officer (ODCIO)	4
About Account Numbers	4
About Userids (“Registered Initials”)	4
About RACF Passwords.....	5
Do You Have a Safe Computing Environment?	5
About Security Investigators	6
DEREGISTRATION OFFICIALS	7
Appointment of Deregistration Officials	7
Responsibilities of Deregistration Officials	7
Working with Account Sponsors.....	8
USING WEB SPONSOR.....	9
What is Web Sponsor?	9
Web Sponsor for Deregistration Officials	9
ACCOUNT SPONSORS	11
Importance of Account Sponsors	11
Responsibilities of Account Sponsors	11
Web Sponsor for Account Sponsors.....	13
OTHER IMPORTANT ISSUES	15
ONGOING TRAINING.....	16
ORDERING DOCUMENTATION	16

EXECUTIVE SUMMARY

The institutes and centers (ICs) of the National Institutes of Health (NIH) maintain sensitive financial systems that require strong security procedures and sound management practices. Among the important financial and management controls is the deregistration of unauthorized users, such as those NIH employees and contractors who leave the NIH or transfer between ICs. Deregistration denies the unauthorized user access to the computing services provided by the Center for Information for Technology (CIT) — specifically from the MVS Enterprise System and its operating environment, which includes the Administrative Data Base System (ADB). Denying access to employees and contractors who have left the IC is a good management practice: it prevents unauthorized access to IC data, and the resulting potential resource cleanup can save IC funds by avoiding unnecessary computer charges.

The deregistration process contains two phases. The first is to deny access of unauthorized personnel from financial applications and the systems they run on. The second involves the cleanup of resources the person utilized (which is the responsibility of the account sponsor, not the deregistration official).

This manual provides the deregistration guidelines required for deregistration officials and account sponsors to ensure that their CIT registered users — authorized to specific accounts — have the correct authority to expend IC monies. The manual also provides an introduction to the computing tool Web Sponsor.

We recommend that this manual be used as a training guide for new staff between formal training offerings, or in place of training offerings when resources are scarce.

Note for Non-NIH Users:

The terms “Executive Officer” or “EO” may be thought of as a “Program Official” or “Security Officer” for non-NIH agencies. Similarly, the term “IC” (for institute or center) may be thought of as a non-NIH agency (e.g., Nuclear Regulatory Commission).

The procedures described in this publication are the same for both NIH users and non-NIH users.

May 2000

ORIENTATION

About the Center for Information Technology (CIT)

CIT provides, coordinates, and manages information technology and works to advance computational science. To accomplish this mission, it provides a variety of data processing services on a cost-recovery basis to the NIH and other government agencies. CIT supports the NIH's research and management programs with efficient, cost-effective information systems, networking services, and telecommunications services. For more information about CIT's mission, visit the CIT home page at <http://cit.nih.gov>.

About the Office of the Deputy Chief Information Officer (ODCIO)

The ODCIO advises the Chief Information Officer (CIO) on the direction and management of significant NIH IT program and policy activities under relevant Federal statutes, regulations and policies. It also develops, implements, manages, and oversees NIH IT activities related to IT legislation, regulations, and NIH and other Federal policies.

The ODCIO directs NIH's IT capital planning processes with regard to major IT investments, and provides leadership to NIH ICs to enhance and strengthen their IT program management so they comply with legislative and policy requirements. The ODCIO serves as the principal NIH liaison to the DHHS, its OPDIVs, and other Federal agencies on IT matters. In addition, the ODCIO identifies critical IT issues and analyzes, plans, leads, and manages the implementation of special DHHS or Federal initiatives as they relate to the management of NIH's IT resources. The ODCIO also collaborates with NIH managers responsible for IT-related functions.

About Account Numbers

Anyone who wishes to use the NIH Computer Center services must first obtain a CIT account. The appropriate account authorization forms are available from the Technical Assistance and Support Center (TASC). These forms are also used to register for a locked output box. The account number is a four-character combination of letters or numbers used to access the system and for accounting purposes; it maps to a Common Account Number (CAN). Persons who are already registered users can request account authorization forms for the MVS system via Web Sponsor.

About Userids ("Registered Initials")

In addition to the account number, each customer will be issued a userid (also known as "registered initials"). A userid may be authorized for use with one or several account numbers. An account may have one or many authorized users.

Userids are the identifiers for an individual users. The userid is composed of three characters, with digits also permitted as the second or third characters. (Dollar signs (\$) are also permitted.)

Users and account sponsors are responsible for the proper professional use of their accounts and userids and the government facilities accessed through them. Users should be individually

registered and should not allow their userid to be used by anyone else. Use of computer time for such things as games, solitaire, personal records, “Quicken,” etc. is illegal. For further information see the *NIH Computer Center User’s Guide*, which can be ordered from TASC, or by visiting the Web page <http://publications.cit.nih.gov>.

About RACF Passwords

Resource Access Control Facility (RACF) passwords are used to gain access to the MVS Enterprise System (e.g., TSO, WYLBUR). All users are automatically registered to RACF when they obtain their userid. Users need only specify the RACF password that is in effect for their userid, to gain access to the MVS Enterprise System. RACF passwords are comprised of 4-8 characters (alphanumeric and national characters) and expire every six months — whether or not the userid has been in use. The expiration policy complies with evolving regulations for computer security at the NIH. *Never* share your password with other individuals, and remember to change it regularly. Passwords can be changed through CIT’s Web RACF facility. Consult the *NIH Computer Center User’s Guide* for more information on various types of userids and for more about RACF.

The DHHS Information Resource Management (IRM) policy requires data centers to provide access-control software to users for protection against unauthorized access to computer facilities. The NIH Computer Center supports RACF for access security and to allow users to maintain additional data protection. All account/initial combinations are automatically registered to RACF for access protection. The CIT Training Program offers classes on RACF. Visit the training home page at <http://training.cit.nih.gov> and register online.

Account sponsors may use Web Sponsor to reset forgotten RACF passwords. Password resets in Web Sponsor are effective immediately. The CIT security investigators can also reset passwords; these resets are usually effective within 24 business hours.

Do You Have a Safe Computing Environment?

Protect your account; change your RACF passwords frequently. The NIH CIT recommends changing passwords at least once a month. Even though NIH Computer Center output does not divulge any password information, security can be compromised over time in subtle ways (e.g., workstations that cannot mask passwords that are entered when signing on to an application or by users who post passwords on “post-its” near workstations).

Be particularly cautious about revealing your RACF password to someone on the telephone. If you feel your password has been compromised and others have signed on to the MVS Enterprise System with your userid, call TASC at (301) 594-6248.

We recommend that passwords consist of both letters and numbers.

When logging on and prompted for a RACF password, it is possible that a simple typing error could generate a security message such as INCORRECT RACF PASSWORD (RECORDED IN SECURITY LOG). While typing errors are expected, users should not attempt to enter the RACF password more than three or four times. After that, the account sponsor should be contacted to determine if the password has been reset for some reason. Users should never try to guess a password that they have forgotten. Instead, the account sponsor should be asked to reset the

password to a known value. As a last resort, CIT security investigators can reset the password within 24 business hours by sending a fax to (301) 496-6905.

Repeated password entry errors are logged in Computer Center security logs, and can trigger a security violation. CIT then revokes the use of the userid until the investigation is completed. For more information on security violation procedures at CIT, refer to the *NIH Computer Center User's Guide*.

About Security Investigators

Security investigators are CIT staff specifically assigned to investigate apparent security violations. If CIT observes or perceives possible security violations, the CIT security investigators will contact the account sponsors of the account that is suspected.

The CIT security investigators offer consulting to help users address and/or avoid security problems in the use of CIT-provided services. Please call TASC and ask to consult with a security investigator.

DEREGISTRATION OFFICIALS

Appointment of Deregistration Officials

Deregistration officials for the NIH are appointed by the IC Executive Officers. For non-NIH Federal agencies, the appointments are made by an agency official responsible for account maintenance, by a program manager or by a security official. These executive officers and agency officials are also responsible for ensuring that the deregistration officials chosen are qualified people. When a deregistration official leaves, for whatever reason, the executive officers are responsible for quickly appointing a replacement.

Executive officers and program officials can designate/authorize a deregistration official by completing the NIH 1767-5 form, and forwarding it to TASC.

All deregistration officials must obtain “preferred initials” when they are registered. Preferred initials are the userid that will be used to perform deregistration official duties. This userid will be recognized by software at the NIH Computer Center and will provide the proper authorities for all deregistration actions. For further assistance on appointing a deregistration official, please call TASC and ask to speak to someone in Customer Accounts about setting up a deregistration official.

Responsibilities of Deregistration Officials

The ultimate responsibility, within the IC or Federal agency, for the accuracy of computer access information belongs to the deregistration official. Since responsibility for information accuracy involves issues of expenditure of funds, security, and privacy, the deregistration official must always be a government employee.

When new accounts are opened, CIT requires that the paperwork be initialed by the account’s deregistration official, indicating receipt. The deregistration official does *not* approve the account opening, nor is it an authorizing signature. This also ensures that each account opened is assigned a deregistration official.

The deregistration official *must* have a backup — a formally assigned alternate who has the same employment profile described above. Only one primary and alternate deregistration official are permitted for each account, and each must be a registered user of the NIH Computer Center. They should also be authorized to use Web Sponsor, the Computer Center’s account management tool. Web Sponsor can be accessed by visiting <http://silk.nih.gov/sponsor/homepage>. Web Sponsor is discussed later in this document, or for more information, see the *NIH Computer Center User’s Guide*.

It is the deregistration official’s responsibility to ensure that the account sponsors (primary and alternate) have preferred initials. This can be done through Web Sponsor. For more information on preferred initials, see the *NIH Computer Center User’s Guide*, or visit the publications page at <http://publications.cit.nih.gov>.

Deregistration officials are automatically subscribed to *Interface*, the Computer Center's technical newsletter, and are strongly encouraged to renew the subscription on an annual basis. *Interface* will announce any changes at the Computer Center that might affect the role of deregistration officials.

The primary and most crucial responsibility of the deregistration official is to ensure that the employee's RACF password has been reset, or the userid deleted, after the employee has left the IC or agency. This will ensure that sensitive data can not be tampered with after the employee's departure, and satisfies the Office of Inspector General's financial audits.

Working with Account Sponsors

There are account sponsors for all CIT accounts — a primary and backup. The account sponsor is the IC official responsible for the maintenance of the resources that the IC employees and contractors are paying for and using at CIT for a specific account. These responsibilities have been in place for over 25 years, and are fully documented in the *NIH Computer Center User's Guide*, and in this document. CIT requests that IC managers designate account sponsors who are technical adept and are readily accessible to the employees and coworkers who will be authorized to use the CIT account. Account sponsors ***must*** be government employees.

Account sponsors have the primary responsibility for removing departed/inappropriate users from their account. "Clean-up work," (e.g., getting rid of data sets, removing databases, releasing tapes, etc.) is done solely by the sponsors. It is merely the deregistration official's responsibility to ensure that the proper deregistration of departed employees has been completed in a timely manner.

USING WEB SPONSOR

What is Web Sponsor?

Web Sponsor (<http://silk.nih.gov/sponsor/homepage>) is an automated account management tool written by, and supported by, CIT. Web Sponsor facilitates account management procedures for the account sponsors, as well as deregistration officials. Web Sponsor will supply deregistration officials and account sponsors with all the necessary information needed to properly administer their accounts.

Web Sponsor allows deregistration officials and account sponsors to display information about a specific account, all accounts, or all accounts under a specific common account number (CAN). Sponsors and deregistration officials can also reset RACF passwords online, averting the faxing of requests to the security investigators. Passwords that are changed via Web Sponsor are effective immediately.

Web Sponsor for Deregistration Officials

- **Display information for decision making**

Web Sponsor provides several ways to display user information to deregistration officials. It displays all accounts for which the deregistration official is responsible for, as well as the names of sponsors associated with those accounts. These accounts and the associated information can be sorted by the IC name along with the common account number (CAN).

Deregistration officials can also see all accounts (with sponsors) for which a specific userid is registered.

For an employee's name, the deregistration official can see all of the accounts to which the employee is registered (with IC, CAN, and sponsors).

The deregistration official is also able to see all userids registered to one or all of their accounts (complete with address, if needed).

- **Resetting RACF passwords**

Resetting RACF passwords through Web Sponsor causes **immediate** denial to the MVS Enterprise systems. Departing employees or contractors will no longer be able to access systems and data once the password is changed. It is wise to use Web Sponsor and reset the password on the employee's last day. CIT *strongly encourages* that RACF passwords be immediately reset for departing, disgruntled employees or contractors. If this is not done, data may be maliciously altered or destroyed. Password changes are recorded in an auditable log.

RACF passwords for deregistration officials should not be shared under any circumstances because of the ability to reset passwords must not be shared. Inappropriate password

resetting may cause loss or misuse of government resources and damage to critical program applications and/or data.

There is one, and only one, RACF password per userid. The password is ***not*** associated with the account/userid combination. By resetting the RACF password, you are changing it for every account that userid is registered to. CIT does not have a strict policy as to whether a userid can be retained by an individual moving to another IC or agency. This is up to the parties involved. Special consideration is needed, however, before an employee takes his/her userid to a new job where they will also use the NIH Computer Center services.

ACCOUNT SPONSORS

Importance of Account Sponsors

Account sponsors play a vital role in the success of the IC computer applications that run at the NIH Computer Center. How sponsors are appointed is at the discretion of IC management. Because of their importance, each sponsor should have a designated backup, or alternate sponsor, for their accounts. The Center for Information Technology (CIT) has only one regulation on who can be an account sponsor; the person must be a government employee. Since sponsors can be responsible for budgetary and financial issues, the appointed person may not be a contractor. CIT, however, does encourage sponsors to be people who are willing to adapt to technological changes, and are available to the users on the account. They have full responsibility of their CIT accounts.

Account sponsors are urged to take advantage of the wide variety of services described in the *NIH Computer Center User's Guide*, and the extensive classroom training offered in the CIT Computer Training program. Documentation is readily available through the publication ordering facilities at CIT or by visiting <http://publications.cit.nih.gov>.

CIT wants to be kept informed of problems encountered by account sponsors and would like to hear about your concerns. Communication, of course, must always be a two-way street. Occasionally, sponsors will be contacted in order to update information or if a problem arises concerning the user of an account. Be available.

The CIT Technical Assistance and Support Center (TASC) serves as the central point of contact for all CIT accounts and welcomes inquiries from sponsors concerning administrative procedures. If you have a concern about your account or account security, please contact TASC at (301) 594-6248.

Responsibilities of Account Sponsors

- Registering an alternate sponsor (including preferred initials). This person will have the authority to act whenever the account sponsor is unavailable to ensure that the work of the organization will not be disrupted.
- Changing the NIH Common Account Number (CAN) to which the account is charged.
- Authorizing additional users on an account.
- Working with the IC deregistration official to ensure that all registered users are current employees or contractors of the responsible IC; have appropriate, approved access; and have current information on their user's records at CIT (e.g., name, address, phone number).
- Ensuring the appropriate use of federal computing resources by all users authorized on an account.

- Communicating with CIT on matters of security and privacy; reporting any suspected violation of password and keyword privacy to CIT's security personnel.
- Investigation of possible security violations relating to a userid registered to the account sponsor's account.
- Reactivation of a userid on appropriate accounts when security investigations are completed.
- Ensuring that all applications and data under their accounts are appropriately protected using the security facilities provided at the NIH Computer Center.
- Ensuring that users are aware of their responsibilities for data security and access control.
- Determining when accounts are to be deactivated and insuring that all chargeable items (e.g., tapes, publicly-stored data sets, hardware, etc.) and userids are deleted prior to deactivation. (Section 2.2 of the *NIH Computer Center User's Guide* offers more information on terminating use of services.)
- Working with the deregistration officials to deregister IC employees/contractors who leave NIH or transfer between ICs.
- Having the ultimate responsibility for user records and technical requirements needed for the "cleanup" phase of deregistration.
- Reminding users to change their passwords frequently in order to maintain access and data security.
- Obtaining forgotten keywords from the CIT security investigators.
- Resetting RACF passwords for users registered to your accounts.
- Reviewing the accounts and making any appropriate changes to the account information or to the names of the users authorized to use the account.
- Requesting Parachute service, when applicable, for users on your accounts.
- Requesting cable modem access for your users.

Web Sponsor for Account Sponsors

- **Resetting RACF passwords**

Web Sponsor is the most effective tool for resetting RACF passwords. By using Web Sponsor, the account sponsor can reset the password — making it effective immediately. Faxes can be sent to the CIT Security Investigators, and because of the nature of the request, can take up to 24 business hours to be reset.

- **Display and change customer information**

Use these options of Web Sponsor to fully display information about one of your accounts, all of your accounts, or accounts by CAN. Web Sponsor displays users registered to your accounts by userid, or by name, as well as showing address and phone numbers. Display handy tables for your accounts—showing the account title, CAN, account sponsors and deregistration officials, along with their preferred initials.

Account sponsors can change information about users registered to their accounts through Web Sponsor. Although the resetting of RACF password is effective immediately with Web Sponsor, most other requests have to be handled by Customer Accounts in CIT. Web Sponsor generates a “request” to Customer Accounts, and the action is usually processed with 24 business hours. There are some exceptions.

- **Validate, remove, reassign, and request new userids**

One of the more important features of Web Sponsor — sponsors can add new users to their accounts, as well as remove users who have departed or no longer have authorization to use that account. New registered userids may be requested through Web Sponsor for new users to the account, as well as requesting multiple sets for one particular user.

- **Perform Helix/POP/ALW/Parachute registration and deregistration**

Sponsors can register their users for Helix, POP, ALW, and Parachute services via Web Sponsor. See the *NIH Computer Center User's Guide* for services offered only for NIH employees.

- **Authorize cable modem requests**

A new feature for CIT and Web Sponsor — sponsors can request cable modem requests through Web Sponsor. This is another feature that is handled internally by CIT, although the request can be initiated with Web Sponsor.

- **Access the CIT Data Warehouse**

Sponsors can look at their CIT bills for their accounts through Web Sponsor, with a direct link to Data Warehouse (DW). The DW stores information that has been requested by the NIH business community and it is designed primarily to analyze business trends and performance. This system takes advantage of the Microsoft Windows interface, which

provides an intuitive, efficient work environment. It acts as an information warehouse, providing integrated, historical business information from the following legacy systems:

Administrative Database (ADB) - supports administrative and financial management activities

Human Resources Database (HRDB) - provides financial and personnel information on the NIH work force

Central Accounting System (CAS) - provides general accounting/financial information

Information for Management, Planning, Analysis, and Coordination (IMPAC II) - tracks information on the NIH grant application, referral, and review process.

- **Account management**

Use Web Sponsor to change account sponsors, assign an alternate sponsor, display account log and information by account, change the CAN of an account, and close CIT accounts. There is online, comprehensive documentation about Web Sponsor, and also the ability to send e-mail to account sponsors and deregistration officials.

- **Getting help with Web Sponsor**

When help is required with Web Sponsor, simply call TASC at (301) 594-6248 and identify yourself as a deregistration official or an account sponsor.

OTHER IMPORTANT ISSUES

- **Account Sponsors and Deregistration Officials**

During the complete deregistration process, it is extremely important and critical that the account sponsor work with the employee's supervisor, and the departing employee or contractor. The employee or contractor should be very knowledgeable about the data sets and tapes he or she maintains — probably more knowledgeable than the account sponsor. Deleting data sets or releasing tapes with program-critical data could be fatal to the program mission. It is vital that the person leaving is consulted about the data he or she maintains. Critical data should be reassigned to another employee involved in the program prior to termination.

- **Rental Equipment**

Employees may have rental equipment assigned to them, in some instances (e.g., printers, modems, and other communications equipment). During the deregistration process, sponsors should ensure that the employee does not have any equipment assigned to him/her — and if so — see that it is transferred to another employee, or the equipment returned to CIT. For assistance in this matter, call TASC at (301) 594-6248 and ask to speak to someone in Dedicated Equipment Services (DES).

- **Ramifications of Reassigning Userids**

When userids are reassigned (i.e., the userids are given another employee's name), sponsors of the recipient of those userids should be aware of the resulting ramifications. Financial obligations are still incurred when the userids are reassigned. Any data sets, tapes, or other CIT-billable resources are still incurring charges to the account of the recipient. CIT strongly encourages the ICs to carefully review the situation — and see if the userids should be reassigned or just deleted.

- **Output Box Numbers**

An output distribution box may have been assigned to the departing employee, or the employee may have been a courier for the IC. Each output box has an associated box access code (BAC), and most employees or couriers over a period of time, memorize the code. Depending on the nature of the employee's departure, the employee could still try to gain access to the output box. Access to the output box could be of concern if the departing employee left on bad terms. If the deregistration officials or the account sponsors are concerned for the integrity of their data or tapes (items that may appear in the output box), they may call TASC and ask to speak to someone in SOMS about box access codes.

ONGOING TRAINING

Knowledge of current deregistration official and account sponsor responsibilities, along with CIT policies is crucial to each IC and other government agencies who use the NIH Computer Center. The CIT offers training as part of the CIT Computer Training program for account sponsors and deregistration officials. Call TASC at (301) 594-6248 to register for the next available seminar, or register online at **<http://training.cit.nih.gov>**.

ORDERING DOCUMENTATION

Ordering documentation from CIT is as easy as 1-2-double-click. Visit the CIT Web page at **<http://publications.cit.nih.gov>** to go to the publications ordering facility. This facility enables users to order manuals and a sundry of types of documentation from CIT. At this site, users can renew their order subscriptions, cancel subscriptions and examine their documentation profile.

Procedures for Deregistration Officials and Account Sponsors

Document Evaluation

Is the Manual:

	YES	NO
Clear?	<input type="checkbox"/>	<input type="checkbox"/>
Well organized?	<input type="checkbox"/>	<input type="checkbox"/>
Complete?	<input type="checkbox"/>	<input type="checkbox"/>
Accurate?	<input type="checkbox"/>	<input type="checkbox"/>
Suitable for the beginner?	<input type="checkbox"/>	<input type="checkbox"/>
Suitable for the advanced user?	<input type="checkbox"/>	<input type="checkbox"/>

Comments:

Please give page references where appropriate. If you wish a reply, include your name and mailing address.

Send to: Applications Services Branch
 Division of Computer System Services
 National Institutes of Health
 Building 12A, Room 4011
 Bethesda, MD 20892-5607

FAX to: (301) 496-6905

ICD or Agency:
Date Submitted:
Name (Optional):
E-Mail Address:

5/00